ЛЕКЦИЯ 11

ГРУППЫ ПОДСТАНОВОК

ПРОСТОТА ГРУППЫ $\mathbf{A}_n$

ДОКАЗАТЕЛЬСТВО НЕПРОСТОТЫ НЕКОТОРЫХ КОНЕЧНЫХ ГРУПП

ХАРАКТЕРИЗАЦИЯ КОММУТАНТА

ГРУППЫ ПОДСТАНОВОК

Напомним, что мы рассматриваем группу подстановок $\mathbf{S}_n$ с записью умножения слева от аргумента: $(\sigma\tau)(i) = \sigma\big(\tau(i)\big)$.

Заметим, что:

$$(i_1\, i_2\, \ldots\, i_k) = (i_1\, i_k)(i_1\, i_{k-1}) \ldots (i_1\, i_2)$$

(в частности, $(1\,2\,\ldots\,k) = (1\,k)(1\,k{-}1)\ldots(1\,2)$); $(i\,j) = (1\,i)(1\,j)(1\,i)$ для $1 \neq i$, $1 \neq j$.

Нам будут полезны разные системы образующих группы $\mathbf{S}_n$:

$$\mathbf{S}_n = \langle (i\,j),\ i \neq j \rangle = \langle (1\,2), (1\,3), \ldots, (1\,n) \rangle.$$

Лемма 1.

$$\tau(1, 2, \ldots, k)\tau^{-1} = \big(\tau(1), \ldots, \tau(k)\big)$$

$(\tau^{-1}(1, 2, \ldots, k)\tau = (\tau^{-1}(1), \ldots, \tau^{-1}(k))$.

Доказательство. Если $\sigma(i) = j$, $\tau(i) = s$, $\tau(j) = t$, то

$$(\tau\sigma\tau^{-1})(s) = (\tau\sigma\tau^{-1})\big(\tau(i)\big) = (\tau\sigma)(i) = \tau(j) = t. \qquad \square$$

Теорема 1. *Две подстановки $\sigma, \gamma \in \mathbf{S}_n$ сопряжены тогда и только тогда, когда они имеют одинаковое цикловое разложение.*

Доказательство.

1) Если $\gamma = \tau\sigma\tau^{-1}$ и $\sigma = \sigma_1 \dots \sigma_r$ — разложение подстановки σ в произведение циклов с непересекающимися орбитами, то

$$\gamma = (\tau\sigma_1\tau^{-1})(\tau\sigma_2\tau^{-1}) \dots (\tau\sigma_r\tau^{-1}),$$

$\{\tau\sigma_i\tau^{-1}\}$ — циклы, орбиты которых являются образами орбит циклов σ_i, и поэтому эти орбиты дают разбиение множества $\{1, 2, \dots, n\}$. Таким образом, подстановки γ и σ имеют одинаковые цикловые разложения.

2) Если γ и σ имеют одинаковое цикловое разложение, то соответствие между элементами соответствующих орбит приводит нас к биекции τ, т. е. $\sigma \in \mathbf{S}_n$, для которой $\gamma = \tau\sigma\tau^{-1}$. □

Лемма 2. *Для циклов длины* 2 τ_1, τ_2 (*т. е. для транспозиций*) *группы* $\mathbf{S}_n$ *при* $n \geqslant 3$ *произведение* $\tau_1\tau_2$ — *либо* 3*-цикл, либо произведение двух* 3*-циклов.*

Доказательство.

Случай 1. Если $\tau_1 = \tau_2$, то

$$\tau_1\tau_2 = \tau_1^2 = e = (i\,j\,k)(k\,j\,i).$$

Случай 2. $\tau_1 \neq \tau_2$.

2а) орбиты пересекаются (по одному элементу i):

$$(i\,k)(i\,l) = (i\,l\,k),$$

здесь $k \neq l$.

2б) Орбиты транспозиций τ_1 и τ_2 не пересекаются:

$$(i\,j)(k\,l) = (i\,l\,j)(i\,l\,k). \qquad \square$$

Теорема 2. $\mathbf{A}_n = \langle\{(i\,j\,k)\}\rangle = \langle(1\,2\,3), (1\,2\,4), \ldots, (1\,2\,n)\rangle$ *при* $n \geqslant 3$.

Доказательство.

1) Если $\sigma \in \mathbf{A}_n$, $n \geq 3$, то $\sigma = \tau_1 \ldots \tau_{2m}$, где τ_i — транспозиция (цикл длины 2). Так как $\tau_{2i-1}\tau_{2i}$ — или 3-цикл, или произведение двух 3-циклов, то

$$\mathbf{A}_n = \langle\{(i, j, k)\}\rangle.$$

2)

$$\begin{aligned}(i\,j\,k) &= (1\,2\,i)(2\,j\,k)(1\,2\,i)^{-1};\\ (2\,j\,k) &= (1\,2\,j)(1\,2\,k)(1\,2\,j)^{-1};\\ (1\,j\,k) &= (1\,2\,k)^{-1}(1\,2\,j)(1\,2\,k).\end{aligned}$$

□

Упражнение 1. $\mathbf{A}_5 = \langle(2\,5\,4), (1\,2\,3\,4\,5)\rangle$.

Теорема 3.

1) $[\mathbf{S}_2, \mathbf{S}_2] = \{e\}$; $[\mathbf{S}_n, \mathbf{S}_n] = \mathbf{A}_n$ *при* $n \geqslant 3$.

2) $[\mathbf{A}_3, \mathbf{A}_3] = \{e\}$; $[\mathbf{A}_4, \mathbf{A}_4] = \mathbf{V}_4$; $[\mathbf{A}_n, \mathbf{A}_n] = \mathbf{A}_n$ *при* $n \geqslant 5$.

Доказательство.

1) Так как $[a, b] = a^{-1}b^{-1}ab$ для $a, b \in \mathbf{S}_n$ всегда является четной подстановкой, то $[\mathbf{S}_n, \mathbf{S}_n] \subseteq \mathbf{A}_n$.

Так как $\mathbf{A}_n = \langle\{(i\,j\,k)\}\rangle$ и

$$(i\,j\,k) = (i\,j)(i\,k)(i\,j)(i\,k) = [(i\,j), (i\,k)],$$

то $\mathbf{A}_n \subseteq [\mathbf{S}_n, \mathbf{S}_n]$.

2а) Так как

$$[(i\,j\,k), (i\,j\,l)] = (k\,j\,i)(l\,j\,i)(i\,j\,k)(i\,j\,l) = (i\,j)(k\,l),$$
$$[(i\,j\,k), (i\,l\,j)] = (k\,j\,i)(j\,l\,i)(i\,j\,k)(i\,l\,j) = (i\,k)(j\,l),$$

то $\mathbf{V}_4 \subseteq [\mathbf{A}_4, \mathbf{A}_4]$.

Так как $|\mathbf{A}_4/\mathbf{V}_4| = 12/4 = 3$, то $\mathbf{A}_4/\mathbf{V}_4$ — абелева группа, поэтому $[\mathbf{A}_4, \mathbf{A}_4] \subseteq \mathbf{V}_4$. Итак, $[\mathbf{A}_4, \mathbf{A}_4] = \mathbf{V}_4$.

2б) При $n \geqslant 5$ для $\{i, j, k\}$ найдутся $l, m \notin \{i, j, k\}$, $l \neq m$. Поэтому

$$(i\,j\,k) = (i\,j\,m)(i\,k\,l)(m\,j\,i)(l\,k\,i) = [(m\,j\,i), (l\,k\,i)],$$

таким образом, $\mathbf{A}_n \subseteq [\mathbf{A}_n, \mathbf{A}_n]$, и следовательно, $\mathbf{A}_n = [\mathbf{A}_n, \mathbf{A}_n]$ при $n \geqslant 5$. □

Упражнение 2. Каждый элемент группы $\mathbf{A}_5$ является коммутатором.

ПРОСТЫЕ ГРУППЫ

Группа G называется *простой*, если у нее нет нормальных подгрупп $N \lhd G$, отличных от $\{e\}$ и G.

Замечание 1. Простые абелевы группы — это в точности циклические группы простого порядка. Действительно, в абелевой группе любая подгруппа нормальна. Поэтому простая абелева группа является циклической. В группе $\mathbb{Z}$ много подгрупп, в частности $2\mathbb{Z}$, т. е. она не является простой. Если $G = (a)$, $O(a) = n = kl$, то $(a^k) \subset (a)$, и группа G не является простой. Итак, $G(a)$ — простая группа тогда и только тогда, когда $|G| = \emptyset(a) = p$.

Замечание 2. Если $|G| = p^k$, $k > 1$, — конечная p-группа из p^k, $k > 1$, элементов, то G не является простой. Действительно, $e \neq \mathbf{Z}(G) \lhd G$.

Теорема о классификации конечных простых групп, видимо, завершена, ее полное связное доказательство создается.

Мы докажем теорему о том, что при $n \geqslant 5$ группа $\mathbf{A}_n$ является простой (в частности, $\mathbf{A}_5$ — простая группа).

Лемма 3. *При $n \geqslant 5$ любые два 3-цикла в группе $\mathbf{A}_n$ сопряжены.*

Доказательство. Пусть $\sigma_1 = (1\,2\,3)$, $\sigma_2 = (a\,b\,c) \in \mathbf{A}_n$, $n \geqslant 5$. Найдется $\tau \in \mathbf{S}_n$, для которой $\sigma_2 = \tau(1\,2\,3)\tau^{-1}$.

а) Если $\tau \in \mathbf{A}_n$, то все доказано.

б) Если $\tau \in \mathbf{S}_n \setminus \mathbf{A}_n$, то $\rho = \tau(4\,5) \in \mathbf{A}_n$, $(4\,5) \in \mathbf{C}_{\mathbf{A}_5}\big((1\,2\,3)\big)$. Тогда

$$\rho(1\,2\,3)\rho^{-1} = \tau(4\,5)(1\,2\,3)(4\,5)^{-1}\tau^{-1} = \tau(1\,2\,3)\tau^{-1} = \sigma_2. \qquad \square$$

Лемма 4. *Подстановки вида $(1\,2)(3\,4)$ и $(a\,b)(c\,d)$ сопряжены в $\mathbf{A}_n$ при $n \geqslant 5$.*

Доказательство. Пусть $m = 5$ (отличный от 1, 2, 3, 4). Тогда $(3\,4\,m)(1\,2)(3\,4)(3\,4\,m)^{-1} = (1\,2)(4\,m)$. $\square$

Теорема 4. $\mathbf{A}_5$ — *простая* (*некоммутативная*) *группа.*

Доказательство. Пусть $\{e\} \neq H \lhd \mathbf{A}_5$.

Случай 1. Пусть $(a\,b\,c) \in H$. Тогда и все сопряженные с ним циклы длины 3 лежат в H, а циклы длины три порождают все $\mathbf{A}_5$, поэтому $H = \mathbf{A}_5$.

Случай. 2. $\alpha = (a\,b\,c\,d\,e) \in H$. Тогда

$$(a\,b)(c\,d)(a\,b\,c\,d\,e)(a\,b)(c\,d) = (b\,a\,d\,c\,e) \in H,$$
$$(b\,a\,d\,c\,e)(a\,b\,c\,d\,e) = (b\,e\,d) \in H,$$

и поэтому (случай 1) $H = \mathbf{A}_5$.

Случай 3. $(a\,b)(c\,d) \in H$. Тогда

$$(a\,b\,c\,e\,d) = (d\,e)(a\,c)(c\,d)(a\,b) \in H,$$

и (случай 2) поэтому $H = \mathbf{A}_5$. □

ПРОСТОТА ГРУППЫ $\mathbf{A}_n$

Мы доказываем теорему о том, что при $n \geqslant 5$ группа $\mathbf{A}_n$ является простой.

Теорема 5. $\mathbf{A}_n$, $n \geqslant 5$, — *простая* (*некоммутативная*) *группа.*

Доказательство. Пусть $\{e\} \neq H \lhd \mathbf{A}_n$.

Если $\sigma = (a\,b\,c) \in H$, то теорема доказана, так как циклы длины три сопряжены в A_n, $n \geqslant 5$, и порождают A_n.

Пусть H содержит некоторую подстановку σ, в разложении которой на непересекающиеся циклы есть цикл длины $\geqslant 4$, т. е. $\sigma = (a\,b\,c\,d\,\ldots)\sigma_2 \ldots \sigma_k$.

Тогда

$$\sigma' = (a\,b\,c)\sigma(c\,b\,a) = (a\,b\,c)(a\,b\,c\,d\,\ldots)(c\,b\,a)\sigma_2 \ldots \sigma_k = \\ = (b\,c\,a\,d\,\ldots)\sigma_2 \ldots \sigma_k \in H,$$

откуда

$$\sigma'\sigma^{-1} = (b\,c\,a\,d\,\ldots)(a\,b\,c\,d\,\ldots)^{-1} = (b\,d\,a) \in H,$$

т.е. $H = \mathbf{A}_n$.

Таким образом, мы можем считать, что в подгруппе H все подстановки при разложении в произведение непересекающихся циклов имеют только циклы длин два и три.

Если подстановка $\sigma \in H$ состоит не только из циклов длины три, то в ее разложении есть по крайней мере две траспозиции (так как она четна):

$$\sigma = (a\,b)(c\,d)\sigma_3 \ldots \sigma_k.$$

В этом случае

$$\sigma' = (a\,b\,c)\sigma(c\,b\,a) = (a\,b\,c)(a\,b)(c\,d)(c\,b\,a)\sigma_3 \ldots \sigma_k = \\ = (a\,d)(c\,b)\sigma_3 \ldots \sigma_k \in H,$$

откуда в H содержится подстановка $\sigma'\sigma^{-1}$, равная $(a\,c)(b\,d)$.

Таким образом, подгруппа H содержит все пары непересекающихся транспозиций, которые порождают $\mathbf{A}_n$.

Остался только случай, когда σ есть произведение непересекающихся циклов длины три, где циклов в разложении больше одного:

$$\sigma = (a\,b\,c)(d\,e\,f)\sigma_3 \ldots \sigma_k \in H.$$

Тогда

$$\sigma' = (b\,c\,d)\sigma(d\,c\,b) = (b\,c\,d)(a\,b\,c)(d\,e\,f)(d\,c\,b)\sigma_3 \ldots \sigma_k = \\ = (a\,c\,d)(b\,e\,f)\sigma_3 \ldots \sigma_k \in H,$$

после чего

$$\sigma'\sigma^{-1} = (a\,c\,d)(b\,e\,f)(c\,b\,a)(f\,e\,d) = (a\,d\,b\,c\,e) \in H,$$

откуда по предудыщему $H = \mathbf{A}_n$. □

ПРИМЕНЕНИЕ ТЕОРЕМ СИЛОВА ДЛЯ ДОКАЗАТЕЛЬСТВА НЕПРОСТОТЫ КОНЕЧНОЙ ГРУППЫ

Лемма 5. *Не существует неабелевых простых групп G порядка $|G| = p^l m$, где p — простое число, p не делит m, p^l не делит $(m-1)!$.*

Доказательство. Допустим противное, пусть G — такая группа.

Тогда G содержит силовскую p-подгруппу S,

$$|S| = p^l, \quad (G : S) = m.$$

Так как конечные неабелевы p-группы не являются простыми (центр является нетривиальной нормальной подгруппой), то можно считать, что $m > 1$.

Ясно (действие на множестве смежных классов G по S), что существует гомоморфизм $\varphi\colon G \to \mathbf{S}_m$ такой, что $\ker\varphi \subseteq S$.

Так как G — простая группа, то $\ker\varphi = \{e\}$, т. е. φ — инъекция.

Поэтому $G \cong \varphi(G) \subseteq \mathbf{S}_m$.

По теореме Лагранжа $p^l m \mid m!$, следовательно, $p^l \mid (m-1)!$, что противоречит нашему предположению. □

Лемма 6. *Если p — простое число, G — конечная p-группа и $|G| > p$, то группа G не является простой.*

Доказательство. Центр $\mathbf{Z}(G)$ нетривиален, при этом $\mathbf{Z}(G) \lhd G$.

Если $\mathbf{Z}(G) \neq G$, то группа G не является простой.

Если $\mathbf{Z}(G) = G$, то G — абелева группа. Если она простая, то $|G| = p$, что противоречит нашему предположению. □

Теорема 6. *Среди конечных групп G, порядок которых меньше чем 60, $|G| < 60$, нет неабелевых простых групп.*

Доказательство. В силу двух предшествующих лемм из чисел $2, 3, \ldots, 59$ надо рассмотреть лишь случаи $n = |G| = 30, 40, 56$.

а) Пусть есть простая группа G, $n = |G| = 30 = 2 \cdot 3 \cdot 5$. Пусть S — силовская 5-подгруппа простой группы G, $|S| = 5$. Число r_5 сопряженных силовских 5-подгрупп (как делитель 30 и $r_5 \equiv 1 \pmod 5$) равно 1 или 6. Но если $r_5 = 1$, то $S \lhd G$, что противоречит простоте группы G. Итак, $r_5 = 6$, при этом пересечение любых двух различных силовских 5-подгрупп из пяти элементов каждая равно $\{e\}$. Итак, их объединение содержит 24 неединичных элемента.

Аналогично число r_3 силовских 3-подгрупп равно 10 ($r_3 \neq 1$, r_3 — делитель 30, $r_3 \equiv 1 \pmod 3$), в их объединении 20 неединичных элементов.

Так как $24 + 20 = 44 > 30$, то получаем противоречие. Итак, группа G с $|G| = 30$ не может быть простой.

б) Пусть есть простая группа G, $n = |G| = 40 = 2^3 \cdot 5$. Пусть S — силовская 5-подгруппа группы G. Так как $r_5 = 1$ ($r \mid 40$, $r \equiv 1 \pmod 5$), то $P \lhd G$, и поэтому группа G не может быть простой.

в) Пусть есть простая группа G, $n = |G| = 56 = 2^3 \cdot 7$. Пусть S — силовская 7-подгруппа группы G. Так как $r_7 = 8$ ($r_7 \mid 56$, $r_7 \equiv 1 \pmod 7$) и пересечение любых двух различных подгрупп из семи элементов равно $\{e\}$, то их объединение содержит 48 неединичных элементов.

Силовская 2-подгруппа содержит восемь элементов, поэтому $48 + 8 = 56 = |G|$, но $r_8 > 1$ (если $r_8 = 1$, то эта силовская подгруппа из восьми элементов нормальна, что противоречит простоте нашей группы G), однако для неединичных элементов второй силовской 2-подгруппы в нашем балансе подсчета элементов уже нет места. Получили противоречие. $\square$

ХАРАКТЕРИЗАЦИЯ КОММУТАНТА

Напомним определение коммутанта $G' = [G, G]$ группы G:

$$G' = [G, G] = \langle [x, y] = x^{-1}y^{-1}xy \mid x, y \in G \rangle,$$

т. е. коммутант — это подгруппа группы G, порожденная всеми коммутаторами.

Поскольку $[x, y]^{-1} = [y, x]$, коммутант G' совпадает с совокупностью всех конечных произведений коммутаторов.

Лемма 7. *Коммутант G' — нормальная подгруппа группы G.*

Фактор-группа $G/G' = G^{\mathrm{ab}}$ — абелева группа, обладающая следующими универсальным свойством (здесь $\pi = \pi_{G'} \colon G \to G/G'$ — канонический гомоморфизм, при котором $\pi(g) = gG'$): для всякого гомоморфизма f из группы G в абелеву группу A существует и единственный гомоморфизм $f' \colon G/G' \to A$, для которого $f = f'\pi$.

Доказательство. Так как для $x, y \in G$ имеем

$$f([x,y]) = [f(x), f(y)] = e_A$$

(f — гомоморфизм групп, A — коммутативная группа), то $f(G') = e_A$, т. е. $G' = \ker \pi \subseteq \ker f$.

Полагая $f'(gG') = f(g)$, видим, что:

1) это отображение определено корректно

$$(gG' = hG' \implies g^{-1}h \in G' \subseteq \ker f \Rightarrow$$
$$\Rightarrow f(g)^{-1}f(h) = f(g^{-1})f(h) = f(g^{-1}h) = e_A \implies f(g) = f(h));$$

2) $f'(gG'hG') = f'(ghG') = f(gh) = f(g)f(h) = f'(gG')f'(hG')$ т. е. f' — гомоморфизм групп;

3) ясно, что $f = f'\pi$, поскольку $f'\pi(g) = f'(gG') = f(g)$ для всех $g \in G$. Это соображение — одна из форм теоремы о гомоморфизме (теорема о факторизации). □

Следствие 1. *Коммутант группы G — это наименьшая нормальная подгруппа в G, фактор по которой абелев.*

ПРИМЕРЫ КОММУТАНТОВ

Пример 1. Коммутант группы $\mathbf{S}_n$ — это группа $\mathbf{A}_n$ для любого $n \geqslant 2$.

Доказательство. Действительно, коммутатор любых двух подстановок является четной подстановкой, поэтому $\mathbf{S}'_n \subseteq \mathbf{A}_n$. С другой стороны, мы показывали выше, что любой цикл длины три является коммутатором:

$$(ijk) = (jk)(ik)(jk)(ij) = [(jk), (ij)],$$

а циклы длины три порождают $\mathbf{A}_n$. □

Пример 2. Коммутант группы $\mathbf{A}_n$ равен:
— $\{e\}$ при $n \leqslant 3$;
— $\mathbf{V}_4$ при $n = 4$;
— $\mathbf{A}_n$ при $n \geqslant 5$.

Пример 3. Коммутант группы кватернионов $\mathbb{Q}_8$ — это ее центр $\{\pm 1\}$.

Доказательство. Действительно, центр группы $\mathbb{Q}_8$ является нормальной подгруппой, фактор по которой абелев (так как состоит из четырех элементов).

С другой стороны, коммутант не может быть меньше центра, так как группа $\mathbb{Q}_8$ не является абелевой. □

Пример 4. Коммутант группы движений “четноугольника”

$$\mathbf{D}_{2k} = \langle a, b \mid a^{2k} = b^2 = e, bab^{-1} = a^{-1} \rangle$$

— это подгруппа $\langle a^2 \rangle$.

Доказательство. Так как

$$[a, b] = aba^{-1}b^{-1} = a^2,$$

то $\langle a^2 \rangle \subseteq \mathbf{D}'_{2k}$. Значит, искомый коммутант не меньше, чем $\langle a^2 \rangle$.

С другой стороны, данная подгруппа нормальна (простая проверка), фактор-группа содержит четыре элемента, т.е. абелева. Значит, это коммутант. □

Упражнение 3. Найдите коммутант правильного “нечетноугольника” $\mathbf{D}_{2n+1}$.